目次

はじめに

このたびは弊社の FMV パソコン（以降、パソコン本体）をご購入いただき、まことにありがとうございます。
本書は、パソコン本体に搭載されているセキュリティチップ（以降、本製品）の基本的な取り扱い、セキュリティチップを利用するためのソフトウェアのインストール、およびアプリケーションの設定と使い方について説明しています。
ご使用になる前に本書およびパソコン本体のマニュアルをよくお読みになり、正しい取り扱いをされますようお願いいたします。

2005 年 4 月

■ セキュリティ機能について

セキュリティ機能は完全な認証照合、データやハードウェアの保護を保証するものではありません。当社は、お客様がセキュリティ機能を使用されたこと、または使用できなかったことによって生じるいかなる損害に関しても、一切の責任を負いかねますのであらかじめご了承ください。

本書の表記

本文中に記載されている記号には、次のような意味があります。

記号	意味
重要	お使いになる際の注意点や、してはいけないことを記述しています。必ずお読みください。
POINT	操作に関連することを記述しています。必要に応じてお読みください。
→	参照ページや参照マニュアルを示しています。

■ コマンド入力（キー入力）

CD-ROM ドライブのドライブ名を、［CD-ROM ドライブ］で表記しています。入力の際は、お使いの環境に合わせて、ドライブ名を入力してください。
例：[CD-ROM ドライブ]：¥setup.exe

■ 連続する操作の表記

本文中の操作手順において、連続する操作手順を、「→」でつなげて記述しています。

例：　「スタート」ボタンをクリックし、「プログラム」をポイントし、「アクセサリ」をクリックする操作

↓

「スタート」ボタン→「プログラム」→「アクセサリ」の順にクリックします。

また、本文中の操作手順において、操作手順の類似しているものは、あわせて記述しています。

例：　「スタート」ボタン→「(すべての) プログラム」→「アクセサリ」の順にクリックします。

■画面例およびイラストについて

表記されている画面およびイラストは一例です。お使いの機種やモデルによって、実際に表示される画面やイラスト、およびファイル名などが異なることがあります。また、このマニュアルに表記されているイラストは説明の都合上、本来接続されているケーブル類を省略していることがあります。

■製品の呼び方

本文中の製品名称を、次のように略して表記します。
なお、本書ではお使いの機種、または OS 以外の情報もありますが、ご了承ください。

<table>
<tr><th>製品名称</th><th colspan="4">本文中の表記</th></tr>
<tr><td>FMV-W5200</td><td>W5200</td><td rowspan="4">FMV-ESPRIMO</td><td colspan="2" rowspan="13">パソコン本体</td></tr>
<tr><td>FMV-E5200</td><td>E5200</td></tr>
<tr><td>FMV-D5200</td><td>D5200</td></tr>
<tr><td>FMV-K5200</td><td>K5200</td></tr>
<tr><td>FMV-X8200</td><td>X8200</td><td rowspan="9">FMV-LIFEBOOK</td></tr>
<tr><td>FMV-E8300</td><td>E8300</td></tr>
<tr><td>FMV-E8200</td><td>E8200</td></tr>
<tr><td>FMV-C8200</td><td>C8200</td></tr>
<tr><td>FMV-S8305</td><td>S8305</td></tr>
<tr><td>FMV-S8205</td><td>S8205</td></tr>
<tr><td>FMV-S8300</td><td>S8300</td></tr>
<tr><td>FMV-S8200</td><td>S8200</td></tr>
<tr><td>FMV-B8200</td><td>B8200</td></tr>
<tr><td>Microsoft® Windows® XP Professional</td><td colspan="2">Windows XP Professional</td><td rowspan="2">Windows XP</td><td rowspan="3">Windows 注</td></tr>
<tr><td>Microsoft® Windows® XP Home Edition</td><td colspan="2">Windows XP Home Edition</td></tr>
<tr><td>Microsoft® Windows® 2000 Professional</td><td colspan="3">Windows 2000</td></tr>
<tr><td>Microsoft® Internet Explorer</td><td colspan="4">Internet Explorer</td></tr>
<tr><td>Microsoft® Word</td><td colspan="4">Word</td></tr>
<tr><td>Microsoft® Outlook®</td><td colspan="4">Outlook</td></tr>
<tr><td>Microsoft® Outlook® Express</td><td colspan="4">Outlook Express</td></tr>
<tr><td>Netscape® または Netscape® Communicator</td><td colspan="4">Netscape</td></tr>
</table>

注：Windows XP/2000 のように併記する場合があります。

商標および著作権について

Microsoft、Windows は、米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。
Netscapeは、米国およびその他の国におけるNetscape Communications Corporation社の登録商標です。
FeliCa は、ソニー株式会社の登録商標です。
FeliCa は、ソニー株式会社が開発した非接触 IC カードの技術方式です。
その他の各製品名は、各社の商標、または登録商標です。
その他の各製品は、各社の著作物です。

画面の使用に際して米国 Microsoft Corporation の許諾を得ています。

使用上のご注意

■ セキュリティチップで利用する鍵や証明書、パスワードの管理について

セキュリティチップは、複数の鍵や証明書を扱います。これらの鍵や証明書を紛失した場合は、その鍵によって暗号化されたファイル等は読めなくなることがありますので注意してください。またこれらの鍵を利用する際にはパスワードが必要です。パスワードが正しく入力されない場合、鍵が利用できないため紛失時同様その鍵によって暗号化されたファイル等は読めなくなります。

■ セキュリティチップ利用についてのご注意

・本製品で使用するユーティリティおよびアプリケーションをインストールするときには、パソコン本体またはネットワーク上のパソコンに、CD-ROM ドライブが搭載／接続されている必要があります。
・セキュリティチップで鍵を生成する場合、数分かかることがあります。
・Infineon Security Platform ユーティリティについては、Infineon Security Platform ユーティリティのマニュアルを参照してください。
・Broadcom Secure Foundation ユーティリティについては Broadcom Secure Foundation ユーティリティのマニュアルを参照してください。
・SMARTACCESS/Trust アプリケーションについては、SMARTACCESS/Trust アプリケーションのマニュアルを参照してください。

・パソコン本体の修理・保守を依頼する場合は、Trusted ログオンを解除してください。
Trusted ログオンを解除していない場合、修理・保守ができないことがあります。Trusted ログオンを解除するには、以下の手順を行ってください。
  1.「スタート」ボタン→「(すべての) プログラム」→「SMARTACCESS Trust」→「ログオン設定ツール」の順にクリックします。
  「ログオン設定ツール」が表示されます。
  2.「ログオン方法変更」をクリックします。
  3.「Trusted ログオン」の「使用する」のチェックを外し、「OK」をクリックします。
・パソコン本体の修理・保守が行われた場合には、セキュリティ機能が解除されていることがあります。その場合には環境の再構築が必要となります。
・修理・保守を行った場合、その作業内容によっては暗号化されたファイルやメールが復元できなくなる場合があります。

1 概要

■セキュリティチップとは

セキュリティチップは、TCG 注 1 の仕様に基づいた TPM 注 2 と呼ばれる IC チップです。TCG により、個人の権利やプライバシーを保護し、かつ様々なセキュリティを実現することができます。セキュリティチップは、TCG セキュリティの基本機能を提供します。セキュリティチップを搭載したパソコンは、ソフトウェアによる攻撃および物理的な攻撃からデータを保護し、より強固なセキュリティを実現します。

注 1：TCG は Trusted Computing Group の略称です。
TCG は、信頼性と安全性を持った新しいコンピュータをつくるためのオープンな業界仕様を策定する団体です。
（https://www.trustedcomputinggroup.org/）

注 2：TPM は Trusted Platform Module の略称です。

■セキュリティチップの機能

セキュリティチップは、各ユーザに固有の鍵を生成し、証明書を管理します。この鍵と証明書を用いることにより、セキュリティチップは暗号化や認証を行います。セキュリティチップ内に保有する鍵は、取り出すことが不可能なため、鍵の解読ができず、そのため暗号化されたデータや認証は安全に行われます。ユーザはこの鍵と証明書を利用するためのパスワードを設定します。

■セキュリティチップの利用

セキュリティチップを利用するために、次のアプリケーションおよび証明書を使用します。

- Infineon TPM Professional Package（Infineon Securiy Platform）ユーティリティ（W5200 を除く）
- Broadcom Secure Foundation ユーティリティ（W5200 のみ）
- SMARTACCESS/Trust アプリケーション
- VeriSign 証明書

これらのアプリケーションおよび証明書により、以下のことが行えるようになります。

□ IEEE802.1x 認証ファイルの管理（W5200 を除く）

- IEEE802.1x にて利用する証明書をセキュリティチップにて管理することができます。

□ ファイルとフォルダの暗号化 -EFS（Encrypting File System）

ユーティリティでファイルとフォルダの暗号化を設定することにより、EFS による暗号化に利用される鍵をセキュリティチップにて安全に保管します。

重要

- EFS を利用するには、ハードディスクが NTFS でフォーマットされている必要があります。
- Windows XP Home Edition では、EFS は利用できません。
- ハードディスク全体を暗号化することはできません。

□ セキュア E-Mail

ユーティリティで電子メールの保護を設定することにより、E-Mail の暗号用の証明書をセキュリティチップにて安全に管理します。

□ Word マクロへの署名

ユーティリティでセキュリティ機能を設定することにより、Word マクロへの署名をセキュリティチップで安全に保護します。

□ Windows ログオンにセキュリティチップを利用する

SMARTACCESS/Trust で Trusted ログオンを設定することにより、Windows ログオン時のパスワードをセキュリティチップにて安全に保存することができます。

□ パソコンの不正なハードウェアの変更の検出

SMARTACCESS/Trust の「機器監査」機能を利用すれば、Windows ログオン時パソコンの機器構成のチェックを行います。ハードウェア構成または設定が不正に変更されていることを検出した場合は、Windows ログオンを許可しないようにすることができます。

□ ID・パスワード入力をセキュリティチップで管理する

ID・パスワードの入力が必要な以下の場合に、ID・パスワードを SMARTACCESS/Trust に登録しておくと、セキュリティチップによって保護されるため、安全に管理することができます。

・アプリケーションによりポップアップ画面に表示される ID・パスワード入力要求

・Internet Explorer によりホームページに表示される ID・パスワード入力要求

また、一度登録すると、ID やパスワードのフォームは自動で認識され、再び手入力することなく利用できます。

□ シングルサインオンを利用する

SMARTACCESS/Trust にはシングルサインオンの機能があります。一度セキュリティチップのパスワードを入力するか、Trusted ログオンを行えば、SMARTACCESS/Trust が管理する ID やパスワードは自動で入力されます。

□ VeriSign 証明書の利用

セキュリティチップと連携した VeriSign 発行の証明書を、登録した日から 1 年間無料で利用できます。これを利用することにより、例えばセキュア E-mail を利用する際などは、VeriSign 認証局に証明された証明書を利用できるため、より安全なデータを送受信することができます。

POINT

- VeriSign 証明書は、セキュリティチップのユーティリティをインストールし、設定を完了して利用可能にしてからインストールを行ってください。インストールについて詳しくは、「Broadcom セキュリティチップセットアップディスク」内の「¥bcmsw105¥verisign.txt」（W5200 の場合）、または「ドライバーズディスク」内の「¥other¥tpm¥ifxsw20¥verisign.txt」（W5200 以外の場合）をご覧ください。
- VeriSign 証明書は、登録した日から 1 年間利用できます。それ以降は、E-mail などで証明書を利用することはできません。ただし、古いメールなどで利用していた場合には、読むことのみ可能です。
- 1 年間の利用期間終了後もご利用を希望の場合は、弊社担当営業員までご連絡ください。その場合有料による継続となります。

□ 他のセキュリティ機能と連携した利用

セキュリティチップは、他のセキュリティ機能と連携した利用が可能です。連携できるセキュリティ機能には、次のものがあります。

・スマートカード
・指紋センサー
・FeliCa 対応リーダ／ライタ

連携の方法などは、SMARTACCESS/Trust 添付のマニュアルを参照してください。

■ セキュリティチップの管理

セキュリティチップには、セキュリティチップの管理を行う [所有者] とセキュリティチップを使用する [ユーザ] を登録します。
所有者およびユーザは次の鍵および証明書やファイルを作成・利用します。

□ [所有者] が管理するもの

所有者キーと所有者パスワード

所有者は、所有者であることを証明するキーを作成します。この鍵はセキュリティチップにより保護され、所有者パスワードを入力することによって利用することができます。
所有者パスワードは忘れないよう十分注意してください。

自動バックアップファイルと復元用トークン（W5200 を除く）

セキュリティチップで管理しているすべての鍵や証明書のバックアップを行います。
バックアップはスケジュールを設定することにより定時に行うことができます。
セキュリティチップが故障しても、新しいパソコンでこのファイルを用いて復元することにより、以前利用していた暗号化ファイルなどが利用できるようになります。
自動バックアップファイルは、トークンにより暗号化されています。自動バックアップファイルを利用する場合には、トークンファイルとそのパスワードが必要です。トークンファイルを失くしたり、パスワードを忘れたりしないよう注意して管理してください。

パスワードリセットファイルとリセットトークン（W5200 を除く）

ユーザがセキュリティチップのパスワードを忘れた場合に備え、現状のパスワードを新規パスワードに変更することができます。パスワードの変更はユーザが行います。所有者はパスワードリセットファイルを発行することにより、ユーザにパスワード変更の許可を与えます。
パスワードリセットファイルは、トークンにより暗号化されています。パスワードリセットファイルを利用する場合には、トークンファイルとそのパスワードが必要です。トークンファイルを失くしたり、パスワードを忘れたりしないよう注意して管理してください。

緊急時復元用アーカイブファイルと復元用トークン（W5200 のみ）

セキュリティチップで管理している所有者情報のバックアップを行います。
セキュリティチップが故障しても、新しいパソコンでこのファイルを用いて復元することにより、所有者の環境を復元することができます。
緊急時復元用アーカイブファイルは、トークンにより暗号化されています。緊急時復元用アーカイブファイルを利用する場合には、トークンファイルとそのパスワードが必要です。トークンファイルを失くしたり、パスワードを忘れたりしないよう注意して管理してください。

□［ユーザ］が管理するもの

ユーザーキーとユーザーキーパスワード

ユーザはセキュリティチップを利用する際、ユーザーキーを作成します。この鍵はセキュリティチップにより保護され、ユーザーキーパスワードを入力することによって利用することができます。鍵を紛失した場合は、それ以前に暗号化していたデータやファイルなどを再び利用することができなくなります。管理には十分注意してください。また、パスワードを忘れた場合も、鍵が利用できなくなるため、それまでに暗号化していたデータやファイルを再び利用することができなくなります。パスワードは忘れないよう十分注意してください。

重要

- W5200 の場合、ユーザーキーパスワードを忘れてしまうと、新たなパスワードに変更できなくなる場合があります。パスワードを忘れないよう十分注意して管理してください。

パスワードリセットファイル（W5200 を除く）

ユーザがセキュリティチップのパスワードを忘れた場合に備え、現状のパスワードを新規パスワードに変更することができます。このため前もってパスワードリセット用のファイルを作成しておきます。

キーのバックアップ

キーを紛失した場合に備え、バックアップファイルを作成することが可能です。バックアップファイルはユーザーキーパスワードによって保護されます。

2 作業の流れ

本製品を使用するまでの手順は次のとおりです。

1 必要なものを用意します。

・パソコン本体
・Broadcom セキュリティチップセットアップディスク（W5200 の場合）
・ドライバーズディスク（W5200 以外の場合）

2 BIOS の設定を変更します。

「BIOS の設定を変更する」（→ P.12）

1. BIOS の「管理者用パスワード」を設定します。
2. セキュリティチップを「使用する」に設定します。

3 ユーティリティをインストールします。

「ユーティリティをインストールする」（→ P.16）

4 ユーティリティの設定を行います。

「ユーティリティの設定を行う」（→ P.17）
「ユーティリティの確認を行う」（→ P.23）

1. 所有者のパスワードを設定します。
2. 緊急時復元用アーカイブを保存します。
3. 緊急時復元用トークンのパスワードを設定します。
4. 緊急時復元用トークンを保存します。
5. 基本ユーザーキーパスワードを設定します。
6. 電子メールの保護と、ファイルとフォルダの暗号化を設定します。
7. 設定の確認を行います。

5 アプリケーションをインストールします。

「アプリケーションをインストールする」（→ P.24）

6 アプリケーションの設定を行います。

「アプリケーションの設定を行う」（→ P.25）

1. Trusted ログオンを設定します。
2. 機器構成を登録し、機器監査を設定します。
3. 一時中止パスワードを設定します。
4. Windows ログオンを Trusted ログオンに変更します。

3 動作条件

本製品をご使用になる前に、次の条件を確認してください。

■ 対応機種／ OS

本製品が搭載されている機種／ Windows XP/2000

POINT

- WEB ページをご覧になるためのアプリケーションとして、Internet Explorer 6.0 以降または Netscape 4.78/7.0 以降が必要です。
- セキュア E-mail を利用するには、Outlook 2000/2002 以降、Outlook Express 6.0 以降、または Netscape 4.78/7.0 以降が必要です。
- Word マクロへの署名を利用するには、Word 2000/2002 以降が必要です。
- VeriSign 証明書を利用するには、Internet Explorer 6.0 または Netscape 4.78/7.0 が必要です。
- SMARTACCESS/Trust での、アプリケーションによりポップアップ画面に表示される ID・パスワード入力要求機能は、Netscape ではお使いになれません。

4 インストールを行う

BIOS の設定を変更する

本製品を使用する前に、必ず BIOS の設定を変更してください。

・「W5200 の場合」（→ P.12）
・「E5200 の場合」（→ P.13）
・「D5200、K5200 の場合」（→ P.14）
・「FMV-LIFEBOOK シリーズの場合」（→ P.15）

POINT

▶ BIOS セットアップについて詳しくは、パソコン本体の『FMV マニュアル』の「BIOS」を参照してください。

■ W5200 の場合

1. **パソコン本体の電源を入れ、BIOS セットアップを起動します。**
BIOS セットアップ画面が表示されます。

2. **Secrity メニューで「Embedded Security Chip」を選択して、【Enter】キーを押します。**
設定変更画面が表示されます。

3. **【↑】キーまたは【↓】キーを押して、「Enabled」に設定します。**

4. **Exit メニューが表示されるまで、何度か【Esc】キーを押します。**

5. **【↑】キーまたは【↓】キーを押して「Save Changes & Exit」を選択し、【Enter】キーを押します。**
「Save Configuration Changes and exit now?」と書かれたウィンドウが表示されます。

6. **【←】キーまたは【→】キーを押して「Yes」を選択し、【Enter】キーを押します。**
BIOS セットアップが終了し、パソコン本体が再起動します。

重要

▶ セキュリティチップの設定を有効にするには、BIOS セットアップ終了後にパソコン本体の再起動が必要です。

■ E5200 の場合

1　パソコン本体の電源を入れ、BIOS セットアップを起動します。

BIOS セットアップ画面が表示されます。
BIOS セットアップで管理者用パスワードを設定済の場合は、手順 7 へ進んでください。設定していない場合には、手順 2 へ進んでください。

重要

- 本製品を使用するには、BIOS セットアップで管理者用パスワードを設定する必要があります。

2　Security メニューで「Set Supervisor Password」を選択して、【Enter】キーを押します。

パスワード入力用のウィンドウが表示されます。

3　8 桁までのパスワードを入力します。

入力できる文字種はアルファベットと数字です。
入力された文字は表示されず、代わりに「＊」が表示されます。

4　パスワードを入力したら、【Enter】キーを押します。

「Confirm New Password」が表示され、パスワードの再入力を求められます。

5　手順 3 で入力したパスワードを再度入力して【Enter】キーを押します。

「Password Installed」と書かれたウィンドウが表示されます。

6　【Enter】キーを押します。

再入力したパスワードが間違っていた場合は、「Passwords do not match!」と書かれたウィンドウが表示されます。【Enter】キーを押して、手順 3 からやり直してください。

7　【↑】キーまたは【↓】キーでカーソルを移動し、「Security Chip」を選択して【Enter】キーを押します。

設定変更画面が表示されます。

8　【↑】キーまたは【↓】キーを押して、「Enabled」に設定します。

9　Exit メニューが表示されるまで、何度か【Esc】キーを押します。

10　【↑】キーまたは【↓】キーを押して「Exit Saving Changes」を選択し、【Enter】キーを押します。

「Save Configuration Changes and exit now?」と書かれたウィンドウが表示されます。

11　【←】キーまたは【→】キーを押して「Ok」を選択し、【Enter】キーを押します。

BIOS セットアップが終了し、パソコン本体が再起動します。

重要

セキュリティチップの設定を有効にするには、BIOS セットアップ終了後にパソコン本体の再起動が必要です。

■ D5200、K5200 の場合

1 パソコン本体の電源を入れ、BIOS セットアップを起動します。

BIOS セットアップ画面が表示されます。
BIOS セットアップで管理者用パスワードを設定済の場合は、手順 7 へ進んでください。設定していない場合には、手順 2 へ進んでください。

重要

- 本製品を使用するには、BIOSセットアップで管理者用パスワードを設定する必要があります。

2 Security メニューで「Set Supervisor Password」を選択して、【Enter】キーを押します。

パスワード入力用のウィンドウが表示されます。

3 8 桁までのパスワードを入力します。

入力できる文字種はアルファベットと数字です。
入力された文字は表示されず、代わりに「■」が表示されます。

4 パスワードを入力したら、【Enter】キーを押します。

「Confirm New Password」にカーソルが移り、パスワードの再入力を求められます。

5 手順 3 で入力したパスワードを再度入力して【Enter】キーを押します。

「Setup Notice」と書かれたウィンドウが表示されます。

6 【Enter】キーを押します。

再入力したパスワードが間違っていた場合は、「Setup Warning」と書かれたウィンドウが表示されます。【Enter】キーを押して、手順 3 からやり直してください。

7 【↑】キーまたは【↓】キーでカーソルを移動し、「Security Chip Setting」を選択して【Enter】キーを押します。

設定変更画面が表示されます。

8 【Space】キーまたは【−】キーを押して、「Security Chip」の項目を「Enabled」に設定します。

9 Exit メニューが表示されるまで、何度か【Esc】キーを押します。

10 【↑】キーまたは【↓】キーを押して「Exit Saving Changes」を選択し、【Enter】キーを押します。

「Save Configuration Changes and exit now?」と書かれたウィンドウが表示されます。

11 【←】キーまたは【→】キーを押して「Yes」を選択し、【Enter】キーを押します。

BIOS セットアップが終了し、パソコン本体が再起動します。

重要

セキュリティチップの設定を有効にするには、BIOS セットアップ終了後にパソコン本体の再起動が必要です。終了メニューで「Exit Saving Changes」を行っただけで電源を切ってしまうと、設定が正しく行われませんのでご注意ください（次回起動時にエラーメッセージが表示されます）。

■ FMV-LIFEBOOK シリーズの場合

1 パソコン本体の電源を入れ、BIOS セットアップを起動します。

BIOS セットアップ画面が表示されます。
BIOS セットアップで管理者用パスワードを設定済の場合は、手順 7 へ進んでください。設定していない場合には、手順 2 へ進んでください。

重要

- 本製品を使用するには、BIOS セットアップで管理者用パスワードを設定する必要があります。

2 セキュリティメニューで「管理者用パスワード設定」を選択して、【Enter】キーを押します。

パスワード入力用のウィンドウが表示されます。

3 8 桁までのパスワードを入力します。

入力できる文字種はアルファベットと数字です。
入力された文字は表示されず、代わりに「■」が表示されます。

4 パスワードを入力したら、【Enter】キーを押します。

「新しいパスワードを確認してください。」にカーソルが移り、パスワードの再入力を求められます。

5 手順 3 で入力したパスワードを再度入力して【Enter】キーを押します。

「セットアップ通知」と書かれたウィンドウが表示されます。

6 【Enter】キーを押します。

再入力したパスワードが間違っていた場合は、「セットアップ警告」と書かれたウィンドウが表示されます。【Enter】キーを押して、手順 3 からやり直してください。

7 【↑】キーまたは【↓】キーでカーソルを移動し、「セキュリティチップ設定」を選択して【Enter】キーを押します。

「セキュリティチップ設定」が表示されます。

8 【Space】キーまたは【−】キーを押して、「セキュリティチップ」の項目を「使用する」に設定します。

9 終了メニューが表示されるまで、何度か【Esc】キーを押します。

10 【↑】キーまたは【↓】キーを押して「変更を保存して終了する」を選択し、【Enter】キーを押します。

「セットアップ確認」と書かれたウィンドウが表示されます。

11 【←】キーまたは【→】キーを押して「はい」を選択し、【Enter】キーを押します。

BIOS セットアップが終了し、パソコン本体が再起動します。

重要

- 「セキュリティチップ」の設定を有効にするには、BIOS セットアップ終了後にパソコン本体の再起動が必要です。終了メニューで「変更を保存する」を行っただけで電源を切ってしまうと、設定が正しく行われませんのでご注意ください（次回起動時にエラーメッセージが表示されます）。

ユーティリティをインストールする

BIOS の設定変更後、パソコン本体が再起動したら、ユーティリティをインストールします。

重要

- ユーティリティをインストールするには、管理者権限で Windows にログオンする必要があります。

POINT

- ユーティリティをインストールする前に、他の使用中のアプリケーションはすべて終了させてください。

1 「Broadcom　セキュリティチップセットアップディスク」（W5200　の場合）、または「ドライバーズディスク」（W5200 以外の場合）をセットします。

POINT

- Windows XP では Windows 起動中に「Broadcom セキュリティチップセットアップディスク」または「ドライバーズディスク」をセットすると、「Windows が実行する動作を選んでください」と表示されます。「キャンセル」をクリックしてください。

2 「スタート」ボタン→「ファイル名を指定して実行」の順にクリックします。

3 「名前」の欄に次のように入力し、「OK」をクリックします。

■ W5200 の場合

[CD-ROM ドライブ]：¥bcmsw105¥install.bat

「Broadcom Secure Foundation(TM) TPM 用の InstallShield ウィザードへようこそ」が表示されます。

■ W5200 以外の場合

[CD-ROM ドライブ]：¥other¥tpm¥ifxsw20¥install.bat

「Infineon TPM Professional Package 用の InstallShield ウィザードへようこそ」が表示されます。

4 「次へ」をクリックします。

「ライセンス契約」が表示されます。

5 「はい」をクリックします。

「ユーザ情報」が表示されます。

6 ユーザ名と所属を入力し、「次へ」をクリックします。

「セットアップタイプ」が表示されます。

POINT

- 所属は省略することもできます。

7 「カスタム」を選択し、「次へ」をクリックします。

「カスタムセットアップ」が表示されます。

8 「次へ」をクリックします。

「プログラムをインストールする準備ができました」と表示されます。

POINT

- 「カスタムセットアップ」では何も変更する必要はありません。

9 「インストール」をクリックします。

インストールが開始します。しばらくして、インストールが終了すると、「InstallShield ウィザードを完了しました」が表示されます。

10 「完了」をクリックします。

メモ帳が表示されます。読み終わったらメモ帳を終了してください。再起動を要求するメッセージが表示されます。

11 「はい」をクリックします。

パソコン本体が再起動します。

ユーティリティの設定を行う

ユーティリティのインストール終了後、パソコン本体が再起動したら、ユーティリティで「プラットフォーム初期化ウィザード」を行い、セキュリティチップの所有者を設定します。その後「ユーザー初期化ウィザード」でユーザの設定を行います。

・「W5200 の場合」(→ P.18)

・「W5200 以外の場合」(→ P.20)

重要

- ユーティリティの設定を行うには、管理者権限を持ったユーザーとして Windows にログオンする必要があります。

■W5200 の場合

1　管理者権限を持ったユーザーとして、Windows にログオンします。

通知領域（Windows XP の場合）またはタスクトレイ（Windows 2000 の場合）の「Broadcom Secure Foundation」アイコンから、「Security Platform が初期化されていません。」というメッセージが表示されます。

2　通知領域（Windows XP の場合）またはタスクトレイ（Windows 2000 の場合）の「Broadcom Secure Foundation」アイコンをクリックします。

メニューが表示されます。

3　「Security Platform の初期化」を選択します。

「Broadcom Secure Foundation (TM) TPM 初期化ウィザードにようこそ」が表示されます。

表示されない場合は、「スタート」ボタン→「(すべての) プログラム」→「Broadcom Security Platform ツール」→「Security Platform 初期化ウィザード」をクリックします。

4　「既存の Security Platform を復元する」にチェックが入っていないことを確認し、「次へ」をクリックします。

「所有者権限の設定」が表示されます。

5　「パスワード」と「パスワードの確認入力」に Security Platform 所有者のパスワードを入力し、「次へ」をクリックします。

「緊急時復元プロセスの設定」が表示されます。

6　「新しい復元用アーカイブを作成する」をチェックして、保存場所を確認し、「次へ」をクリックします。

「Security Platform の緊急時復元用トークンのパスワードを入力」が表示されます。

重要

- 緊急時復元用アーカイブの保存場所は通常、表示されている場所から変更する必要はありません。

7　「パスワード」と「パスワードの確認入力」に緊急時復元用トークンのパスワードを入力し、「次へ」をクリックします。

「復元用トークンの保存」が表示されます。

8　緊急時復元用トークンの保存場所を設定し、「次へ」をクリックします。

「サマリー」が表示されます。

重要

- 保存先は仮の場所が表示されています。緊急時復元用トークンは、リムーバブルドライブなど、パソコン本体とは別の場所に保管できる媒体に保存することをお勧めします。

9　「次へ」をクリックします。

しばらくすると、「ウィザードが正常に終了しました。」が表示されます。

10 「Security Platform ユーザー初期化ウィザードを起動する」をチェックして「完了」をクリックします。

「Broadcom Secure Foundation(TM) TPM ユーザー初期化ウィザードにようこそ」が表示されます。

11 「次へ」をクリックします。

「基本ユーザーキーのパスワード」が表示されます。

12 基本ユーザーキーの「パスワード」と「パスワードの確認入力」に入力し、「次へ」をクリックします。

「設定の確認」が表示されます。

13 「次へ」をクリックします。

しばらくすると、「Security Platform の機能」が表示されます。

14 「電子メールの保護」、「ファイルとフォルダの暗号化 (EFS)」にチェックが入っていることを確認し、「次へ」をクリックします。

「電子メールの保護に関する設定」が表示されます。

重要

- 「電子メールの保護」と「ファイルとフォルダの暗号化 (EFS)」の他に「Personal Secure Drive」が表示されていることがありますが、チェックしないでください。本機能はサポートしていません。
- Windows XP Home Edition をお使いの場合は、「ファイルとフォルダの暗号化 (EFS)」は選択できません。

15 「次へ」をクリックします。

「暗号化証明書」が表示されます。

16 「発行先」が自分になっていることを確認し、「次へ」をクリックします。

「設定の確認」が表示されます。

17 「次へ」をクリックします。

しばらくすると、「ウィザードが正常に終了しました。」が表示されます。

18 「完了」をクリックします。

「今すぐ再起動しますか ?」が表示されます。

19 「はい」をクリックします。

パソコン本体が再起動します。

以上で、Broadcom Secure Foundation ツールによる TCG セキュリティ機能が利用できる環境が整いました。

■W5200 以外の場合

1 管理者権限を持ったユーザーとして、Windows にログオンします。

通知領域（Windows XP の場合）またはタスクトレイ（Windows 2000 の場合）の「Infineon Security Platform」アイコンから、「Security Platform が初期化されていません」というメッセージが表示されます。

2 通知領域（Windows XP の場合）またはタスクトレイ（Windows 2000 の場合）の「Infineon Security Platform」アイコンをクリックします。

メニューが表示されます。

3 「Security Platform の初期化」を選択します。

「Infineon Security Platform 初期化ウィザードへようこそ」が表示されます。

4 「次へ」をクリックします。

「初期化」が表示されます。

5 「新しく Security Platform を初期化する」にチェックが入っていることを確認し、「次へ」をクリックします。

「Security Platform 所有者を作成します。」が表示されます。

6 「パスワード」と「パスワードの確認入力」に Security Platform 所有者のパスワードを入力し、「次へ」をクリックします。

「機能」が表示されます。

7 「自動バックアップ」および「パスワードリセット」にチェックが入っていることを確認し、「次へ」をクリックします。

「自動バックアップ」が表示されます。

8 「バックアップの場所」にバックアップの場所を設定します。自動バックアップのスケジュールを変更する場合は、「スケジュール」をクリックして設定し、「次へ」をクリックします。

「緊急時復元」が表示されます。

重要

- 自動バックアップのアーカイブは大切なファイルです。ハードディスク内の削除されない場所を指定してください。また、保存場所も記憶しておいてください。
- スケジュールで設定された時間にパソコン本体の電源が入っていない場合には、自動バックアップは実行されません。

9 「新しい復元用トークンを作成する」をチェックし、「ファイルの場所」に緊急時復元用トークンの保存場所を設定します。

重要

- 「ファイルの場所」には仮の場所が表示されています。緊急時復元用トークンは、リムーバブルドライブなど、パソコン本体とは別の場所に保管できる媒体に保存することをお勧めします。
- 復元用トークンファイルとトークンアーカイブは紛失、忘却しないよう注意して管理してください。

10 「パスワード」と「パスワードの確認入力」に緊急時復元用トークンのパスワードを入力し、「次へ」をクリックします。

「パスワードリセット」が表示されます。

11 「新しいトークンを作成する」をチェックし、「ファイルの場所」でパスワードリセットトークンの保存場所を設定します。

重要

- 「ファイルの場所」には仮の場所が表示されています。パスワードリセットトークンは、リムーバブルドライブなど、パソコン本体とは別の場所に保管できる媒体に保存することをお勧めします。
- パスワードリセットトークンファイルとトークンアーカイブは紛失、忘却しないよう注意して管理してください。

12 「パスワード」と「パスワードの確認入力」にパスワードリセットトークンのパスワードを入力し、「次へ」をクリックします。

「サマリー」が表示されます。

13 「次へ」をクリックします。

しばらくすると、「ウィザードが正常に終了しました。」が表示されます。

14 「Security Platform ユーザー初期化ウィザードを起動する」をチェックして「完了」をクリックします。

「Infineon Security Platform ユーザー初期化ウィザードへようこそ」が表示されます。

15 「次へ」をクリックします。

「基本ユーザーパスワード」が表示されます。

16 「パスワード」と「パスワードの確認入力」に基本ユーザーパスワードを入力し、「次へ」をクリックします。

「基本ユーザーパスワードリセット」が表示されます。

17 「緊急時の基本ユーザーパスワードのリセットを有効にする」にチェックが入っていることを確認し、「個人シークレットの場所」を設定します。

重要

- 「個人シークレットの場所」には仮の場所が表示されています。個人シークレットファイルは、リムーバブルドライブなど、パソコン本体とは別の場所に保管できる媒体に保存することをお勧めします。

18 「次へ」をクリックします。

「パスワードと認証」が表示されます。

19 「次へ」をクリックします。

しばらくすると、「Security Platform の機能」が表示されます。

20 「電子メールの保護」、「暗号化ファイルシステム（EFS）によるファイルとフォルダの暗号化」にチェックが入っていることを確認し、「次へ」をクリックします。

「電子メールの保護の設定をしてください。」が表示されます。

重要

- 「電子メールの保護」と「暗号化ファイルシステム（EFS）によるファイルとフォルダの暗号化」の他に「Personal Secure Drive」が表示されていることがありますが、チェックしないでください。本機能はサポートしていません。
- Windows XP Home Edition をお使いの場合は、「暗号化ファイルシステム（EFS）によるファイルとフォルダの暗号化」は選択できません。

21 「次へ」をクリックします。

「暗号化証明書」が表示されます。

22 「選択」をクリックします。

「Infineon Security Platform 証明書の選択」が表示されます。

23 「作成」をクリックします。

しばらくすると、証明書が作成されます。

24 リストから「発行先」に表示された自分のユーザ ID を選択し、「選択」をクリックします。

25 「発行先」が自分になっていることを確認し、「次へ」をクリックします。

「設定を確認してください。」が表示されます。

26 「次へ」をクリックします。

しばらくすると、「ウィザードが正常に終了しました。」が表示されます。

以上で、Infineon Security Platform ツールによる TCG セキュリティ機能が利用できる環境が整いました。

ユーティリティの確認を行う

ユーティリティのインストールと設定が完了したら、次の手順で正しく設定されたか確認してください。

■ W5200 の場合

1 **「スタート」ボタン→「(すべての) プログラム」→「Broadcom Security Platform ツール」の「Security Platform 設定ツール」の順にクリックします。**

「Broadcom Secure Foundation(TM) TPM 設定ツール」が表示されます。

2 **「全般」タブをクリックします。**

3 **「Security Platform の状態」が次の状態になっていることを確認します。**

「チップ」:有効
「所有者」:初期化完了
「ユーザー」:初期化完了

4 **「OK」をクリックし、「Broadcom Secure Foundation(TM) TPM 設定ツール」を終了します。**

■ W5200 以外の場合

1 **「スタート」ボタン→「(すべての) プログラム」→「Infineon Secure Platform ソリューション」の「Security Platform を管理します」の順にクリックします。**

「Infineon Security Platform 設定ツール」が表示されます。

2 **「全般」タブをクリックします。**

3 **「Security Platform の状態」が次の状態になっていることを確認します。**

「Chip」:有効
「所有者」:初期化済み
「ユーザー」:初期化済み

4 **「OK」をクリックし、「Infineon Security Platform 設定ツール」を終了します。**

アプリケーションをインストールする

ユーティリティの設定が完了したら、SMARTACCESS/Trust アプリケーションをインストールします。

重要

- アプリケーションをインストールするには、管理者権限を持ったユーザとして Windows にログオンする必要があります。

POINT

- アプリケーションをインストールする前に、他の使用中のアプリケーションはすべて終了させてください。

1 「Broadcom　セキュリティチップセットアップディスク」（W5200　の場合）、または「ドライバーズディスク」（W5200 以外の場合）をセットします。

POINT

- Windows XP では Windows 起動中に「Broadcom セキュリティチップセットアップディスク」または「ドライバーズディスク」をセットすると、「Windows が実行する動作を選んでください」と表示されます。「キャンセル」をクリックしてください。

2 「スタート」ボタン→「ファイル名を指定して実行」の順にクリックします。

3 「名前」の欄に次のように入力し、「OK」をクリックします。

■ W5200 の場合

[CD-ROM ドライブ]：¥satrust¥setup.exe

■ W5200 以外の場合

[CD-ROM ドライブ]：¥other¥tpm¥satrust¥setup.exe

「SMARTACCESS/Trust V1.0L22 をコンピュータにインストールします。」が表示されます。

4 「次へ」をクリックします。

「セットアップは次のフォルダに SMARTACCESS/Trust V1.0L22 をインストールします。」が表示されます。

5 インストール先のフォルダを選択して、「次へ」をクリックします。

インストールが開始されます。
しばらくすると、「SMARTACCESS/Trust V1.0L22 のインストールを完了しました。」が表示されます。

POINT

- インストール先のフォルダは通常、変更する必要はありません。変更すると不都合が発生することもあるため、パソコンに詳しい方以外は変更しないでください。

6 「完了」をクリックします。

再起動を要求するメッセージが表示されます。

7 「はい」をクリックします。

パソコンが再起動します。

アプリケーションの設定を行う

アプリケーションのインストールが終わったら、アプリケーションの設定を行います。
アプリケーションにより Windows のログオンパスワードなどをセキュリティチップに保存するので、パスワードを安全に管理できます。

POINT

- 必ず管理者でログオンしてください。
- 他のアプリケーションはすべて終了させてください。
- 他のセキュリティ機能により Windows ログオンを行っている場合は、その利用を止めてから設定するか、セキュリティチップにて行うのを止めてください。
- アプリケーションの設定について詳しくは、SMARTACCESS/Trust アプリケーションのマニュアルを参照してください。

重要

- 設定の途中で、現在のパソコンの機器構成を登録する作業を行います。
  機器構成を登録すると、現在の BIOS ハードウェア設定などを保存します。登録を行う前に BIOS 設定を含めたハードウェア設定（機器構成）を完了してから行ってください。

1 「スタート」ボタン→「（すべての）プログラム」→「SMARTACCESS Trust」→「ログオン設定ツール」の順にクリックします。

「ログオン設定ツール」が表示されます。

2 ユーザーキーパスワードを入力し「OK」をクリックします。

3 「Trusted ログオン」の「登録」をクリックします。

「Trusted ログオン情報登録」が表示されます。

4 「Windows ログオン」に、Windows ログオン時の「ユーザー名」、「ドメイン名」、「パスワード」、および「パスワードの確認入力」を入力します。

POINT

- ドメインを利用していない場合は「ドメイン名」の入力は不要です。

5 「登録するユーザーのユーザーキーパスワード」に、パスワードを入力し、「OK」をクリックします。

「Trusted ログオン情報を設定しました。」が表示されます。

6 「OK」をクリックします。

「ログオン設定ツール」に戻ります。

□ 機器監査の設定を行う

つづいて、機器監査の設定を行います。機器監査の設定を行わない場合は、「シングルサインオンの設定を行う」（→ P.26）に進んでください。

7 **「Trusted ログオン」の「機器構成設定」をクリックします。**

「Trusted ログオン機器構成情報登録」が表示されます。

8 **「現状登録」をクリックします。**

「現在の機器構成を登録しますか？」が表示されます。

9 **「はい」をクリックします。**

「Trusted ログオン機器構成情報登録」に戻ります。

重要

- Windows が起動される直前の機器構成が登録されます。モバイルマルチベイ／マルチベイの変更（FMV-LIFEBOOK シリーズの場合）など、Windows の起動後に行った機器の変更は登録されませんのでご注意ください。

10 **「起動時に機器監査実行」をチェックします。**

11 **「起動時に機器構成が異なる場合のログオン」を「ログオンしない」にチェックして、「OK」をクリックします。**

「ログオン設定ツール」に戻ります。

重要

- 機器監査で検出されるハードウェアの変更については、「機器監査について」（→ P.39）を参照してください。機器構成を不用意に変更すると、ログオンが行えなくなる可能性がありますので十分にご注意ください。再度、機器構成の変更が必要となった場合は、必ず「起動時に機器監査実行」を一度オフにしてから行ってください。

12 **「一時中止パスワード」をクリックし、パスワードを入力し、「OK」をクリックします。**

「一時中止パスワードを登録しました。」が表示されます。

重要

- 一時中止パスワードは、セキュリティチップに不具合が発生したときなどTrusted ログオンができなくなった場合に、一時的に Windows ログオンに切り替えるための手段です。
- 一時中止パスワードで Windows にログオンしても、セキュリティチップによって暗号化されたファイルなどは、安全に保護されています。これらファイルは、ユーザーキーパスワードを入力するまで見ることができません。

13 **「OK」をクリックします。**

「ログオン設定ツール」に戻ります。

□ シングルサインオンの設定を行う

つづいて、シングルサインオンの設定を行います。シングルサインオンの設定を行わない場合は、手順 16 に進んでください。

14 「その他」の「動作環境設定」をクリックします。

「動作環境設定」が表示されます。

15 「シングルサインオン」の「有効にする」にチェックし、「OK」をクリックします。

「ログオン設定ツール」に戻ります。

16 「ログオン方法変更」をクリックし、「Trusted ログオン」を「使用する」にチェックし、「OK」をクリックします。

「本製品以外のログオン認証が有効になっている場合・・・」の確認画面が表示されます。

17 「OK」をクリックします。

「ログオン方法を変更しました。」が表示されます。

18 「OK」をクリックします。

「ログオン設定ツール」に戻ります。

19 「閉じる」をクリックします。

再起動を要求するメッセージが表示されます。

20 「はい」をクリックします。

パソコンが再起動します。

POINT

- 設定後は、Windows ログオン画面は「ようこそ」表示から「クラシック」表示に切り替わります。
- Windows ログオンの方法は次の手順になります。
  1. Windows を起動後、画面の指示に従い、【Ctrl】+【Alt】+【Del】キーを押します。
     「Trusted ログオン」画面が表示されます。
  2. ユーザー名とユーザーキーパスワードを入力します。
     Windows にログオンします。

5 運用上の注意

セキュリティチップの運用上の注意

セキュリティチップを利用するための環境設定が完了すると、ファイルやフォルダの暗号化、メールの証明書の管理などがより安全な環境で運用することができるようになります。故障や修理などでパソコン本体の設定が変更された場合、セキュリティチップにより保護された情報が利用できなくなることがあります。
これらの場合に備えて、次の点に注意して運用してください。

□ 定期的にセキュリティチップの鍵のバックアップを行う

必ずセキュリティチップによって管理されている鍵のバックアップを行ってください。

重要

- バックアップファイルを紛失したり、パスワードを忘れたりすると、セキュリティチップが利用できなくなります。バックアップファイルやその時に設定したパスワードは、紛失したり忘れたりしないよう注意して管理してください。
  バックアップの方法については、「鍵のバックアップについて」（→ P.29）を参照してください。
- バックアップを行うと、次のファイルとパスワードが生成されます。
  ・W5200 の場合

利用者	ファイル／パスワード	ファイル名
所有者	所有者パスワード	
	緊急時復元用アーカイブ	spemrecarchive.xml
	緊急時復元用トークン	spemrectoken.xml
	トークンパスワード	
	（基本）ユーザーパスワード	
	バックアップファイル	spbackup.xml
ユーザ	（基本）ユーザーパスワード	
	バックアップファイル	spbackup.xml

・W5200 以外の場合

利用者	ファイル	ファイル名
所有者	所有者パスワード	
	システム復旧ファイル	spsystembackup.xml
	緊急時復元用トークン	spemrectoken.xml
	緊急時復元用トークンパスワード	
	パスワードリセットファイル	sppwdresetsecret.xml
	パスワードリセットトークン	sppwdresettoken.xml
	パスワードトークンパスワード	
	（基本）ユーザーパスワード	
ユーザ	（基本）ユーザーパスワード	
	パスワードリセットトークン	sppwdresetsecret.xml
	パスワードトークンパスワード	

▶ 復元作業は、パスワードの入力などが必要なため、弊社で行うことはできません。「鍵の復元について（W5200 の場合）」（→ P.32）または「鍵の復元について（W5200 以外の場合）」（→ P.35）に従って注意して復元してください。

□ 機器監査を行っている場合は、修理またはハードウェア変更を行う前に Trusted ログオンを一時的に解除する

Trusted ログオンを使用する設定にして機器監査を行っている場合、修理したり、ハードウェアの設定を変更したりすると、Windows にログオンできなくなることがあります。
必ず Trusted ログオンを使用しない設定に変更してください。

重要

▶ パソコンの修理またはハードウェアの変更を行う前に、一時的に Trusted ログオンを行わない設定に変更してください。変更方法については、「パソコンの修理について」（→ P.40）を参照してください。

POINT

▶ 次のような状況が起きた場合に、セキュリティチップが利用できなくなると考えられます。
  ・セキュリティチップの故障
  ・ハードディスクのリカバリ
  ・パソコンの部品の交換

鍵のバックアップについて

POINT

▶「バックアップ」とは、前もって新しい環境に引き継ぐための準備をすることです。セキュリティチップの中の鍵を取り出して保存することではありません。

鍵のバックアップは、利用中のセキュリティチップにより保護された環境に何らかの変更があった場合に、以前の環境を引き続き利用するときに必要な準備をするための作業です。

所有者でログオンした時に、通知領域（Windows XP の場合）またはタスクトレイ（Windows 2000 の場合）から表示される内容により、次の手順に従って処理を行ってください。

・「W5200 の場合」（→ P.30）
・「W5200 以外の場合」（→ P.31）

重要

- バックアップ処理は、セキュリティチップを設定した時のパスワードによって保護されています。そのため、セキュリティチップを設定した人が行う必要があります。
- ほとんどの設定は「Security Platform の初期化」時および「Security Platform のユーザ初期化」時に行われます。そのときに作成したファイルを注意して管理する必要があります。また、修理などを行う前に行っておかなければならない作業もあります。手順に従い注意して管理してください。
- 手順に従ってファイルや設定変更を行わない場合、セキュリティチップで管理していた環境が利用できなくなることがあります。
- ここで説明する手順は、セキュリティチップの鍵についてバックアップを行う場合の手順です。暗号化ファイルや証明書、および SMARTACCESE/Trust の設定については行われません。必要に応じて別途バックアップを行ってください。
  SMARTACCESS/Trust のバックアップについては、SMARTACCESS/Trust アプリケーションのマニュアルにある「ログオン情報を移行する」を参照してください。

■ W5200 の場合

所有者はセキュリティチップのバックアップを行う必要があります。
また、各ユーザはユーザーキーのバックアップを行う必要があります。

POINT

- 操作について詳しくは、Broadcom Secure Foundation ツールのマニュアルを参照してください。

□ 所有者が行う作業

所有者が行わなければならない作業は、Security Platform の初期化時の「緊急時復元用アーカイブ」の設定時にほぼ完了しています。「ユーザが行う作業」（→ P.30）を行ってください。

重要

- 「Security Platform の初期化」時に作成した 緊急時復元用トークンとパスワードは大切に管理してください。
  これらを紛失すると復元できません。

□ ユーザが行う作業

1 **通知領域（Windows XP の場合）またはタスクトレイ（Windows 2000 の場合）の「Broadcom Secure Foundation」アイコンをクリックし、表示されるメニューから「Security Platform の管理」を選択します。**

「Broadcom Secure Foundation(TM) TPM 設定ツール」が表示されます。

2 **「バックアップ」タブを選択し、「バックアップ」をクリックします。**

「キーと証明書をバックアップする」が表示されます。

3 **「参照」をクリックし、鍵（ファイル）をバックアップする場所を選択します。**

POINT

- 所有者は、「緊急時復元用アーカイブをバックアップデータに追加」にチェックをしてください。

4 **「次へ」をクリックします。**

「サマリー」が表示されます。

5 **「次へ」をクリックします。**

鍵(ファイル)が保存されると、「ウィザードが正常に終了しました」が表示されます。

6 **「完了」をクリックします。**

■ W5200 以外の場合

所有者はセキュリティチップのバックアップと各ユーザのバックアップを行う必要があります。
各ユーザでバックアップを行う必要はありませんが、復元を行った後、ユーザーキーパスワードを入力する必要があります。

POINT

- 操作について詳しくは、Infineon Security Platform ツールのマニュアルを参照してください。

□ 所有者が行う作業

所有者が行う作業は「Security Platform の初期化」時の「自動バックアップ」の設定時にほぼ完了しています。

重要

- 自動バックアップファイルは、スケジュールで設定した時刻に作成または更新されます。
- スケジュールで設定した時刻にパソコンの電源が入っていなかった場合には、自動バックアップは実行されません。
- すぐにバックアップを行う場合には、次の手順で行います。
  1. 「スタート」ボタン→「ファイル名を指定して実行」の順にクリックします。
  2. 「名前」の欄に次のように入力し、「OK」をクリックします。「Infineon Security Platform ソリューション」のインストール場所を変更した場合は、「参照」をクリックして変更先のフォルダ内にある「SpBackupWz.exe」を指定し、「名前」の欄に表示されるファイル名に続けて「 /backupall」を入力します。
     "C:¥Program Files¥Infineon¥Security Platform Software¥SpBackupWz.exe" /backupall
  3. 「OK」をクリックします。

□ ユーザが行う作業

所有者によって自動バックアップファイルが作成されるため、バックアップなどの準備は必要ありませんが、パスワードを入力する必要があります。
念のためバックアップを行う場合は、次の手順で行います。

重要

- 次の手順では、作業を行うユーザの鍵のみがバックアップされます。所有者用の鍵や他のユーザの鍵はバックアップされません。

1 **通知領域（Windows XP の場合）またはタスクトレイ（Windows 2000 の場合）の「Infineon Security Platform」アイコンをクリックし、表示されるメニューから「Security Platform を管理する」を選択します。**
「Infineon Security Platform 設定ツール」が表示されます。

2 **「バックアップ」タブを選択し、「バックアップ」をクリックします。**
「バックアップ」が表示されます。

3 **「参照」をクリックし、鍵（ファイル）をバックアップする場所を選択します。**

4 **「次へ」をクリックします。**
「サマリー」が表示されます。

5 **「次へ」をクリックします。**
鍵（ファイル）が保存されると、「ウィザードが正常に終了しました。」が表示されます。

6 **「完了」をクリックします。**

鍵の復元について（W5200 の場合）

鍵の復元は、利用中のセキュリティチップにより保護された環境に何らかの変更があった場合に、以前の環境を引き続き利用するための作業です。
所有者はセキュリティチップの復元を行う必要があります。また、各ユーザはユーザーキーの復元を行う必要があります。

POINT

- 操作について詳しくは、Broadcom Secure Foundation ツールのマニュアルを参照してください。

鍵の復元については、どのような状態から復元を行うかによって作業手順が異なります。
所有者でログオンした時に、通知領域（Windows XP の場合）またはタスクトレイ（Windows 2000 の場合）にメッセージが表示されます。表示される内容により、次の手順に従って処理を行ってください。

重要

- 復元処理は、セキュリティチップを設定した時のパスワードによって保護されています。このため、復元処理はセキュリティチップを設定した人が行う必要があります。
- ほとんどの設定は「Security Platform の初期化」時および「Security Platform のユーザ初期化」時に行われます。そのときに作成したファイルを注意して管理する必要があります。また、パソコンの修理などを行う前にしておかなければならない作業もあります。手順に従い注意して管理してください。
- 手順に従ってファイルや設定変更を行わない場合、セキュリティチップで管理していた環境が利用できなくなることがあります。
- ここで説明する手順は、セキュリティチップの鍵について復元を行う場合の手順です。暗号化ファイルや証明書、および SMARTACCESE/Trust の設定については行われません。必要に応じて別途復元を行ってください。
  SMARTACCESS/Trust のバックアップについては、SMARTACCESS/Trust アプリケーションのマニュアルにある「ログオン情報を移行する」を参照してください。

■通知領域またはタスクトレイから「Security Platform が初期化されていません。」と表示された場合

□ 所有者が行う作業

POINT

- 事前に次のものを確認してください。
  - ・所有者パスワード
  - ・緊急時復元用アーカイブ
  - ・緊急時復元用トークンとそのパスワード
- Trusted ログオンを設定している場合は、「一時中止パスワード」にて Windows にログオンする必要があります。

1 パソコンの電源を入れます。

通知領域（Windows XP の場合）またはタスクトレイ（Windows 2000 の場合）の「Broadcom Secure Fondation」アイコンから、「Security Platform が初期化されていません。」と表示されます。

2 通知領域（Windows XP の場合）またはタスクトレイ（Windows 2000 の場合）の「Broadcom Secure Fondation」のアイコンをクリックします。

メニューが表示されます。

3 「Security Platform の初期化」をクリックします。

「Broadcom Secure Fondation(TM) TPM 初期化ウィザードにようこそ」が表示されます。

4 「既存の Security Platform を復元する」にチェックをして、「次へ」をクリックします。

「所有者権限の設定」が表示されます。

重要

- 必ず「既存の Security Platform を復元する」にチェックをしてください。

5 所有者の「パスワード」と「パスワードの確認入力」を入力し、「次へ」をクリックします。

「緊急時復元プロセスの設定」が表示されます。

6 「既存の復元用アーカイブに追加する」をチェックし、「参照」をクリックして緊急時復元用アーカイブの場所を指定します。

重要

- 必ず「既存の復元用アーカイブに追加する」にチェックをしてください。「新しい復元用アーカイブを作成する」を選択すると、新しいアーカイブが以前のアーカイブに上書きされるため、以前の環境を再構築できなくなり、暗号化ファイルなどを見ることができなくなります。

7 「次へ」をクリックします。

「サマリー」が表示されます。

8 「次へ」をクリックします。

「緊急時復元プロセスの準備」が表示されます。

9 「参照」をクリックし、緊急時復元用アーカイブの場所を再び指定して、「次へ」をクリックします。

「緊急時復元用トークンの場所の指定と、パスワードの入力」が表示されます。

10 「参照」をクリックして緊急時復元用トークンの場所を指定します。

11 パスワードを入力し、「次へ」をクリックします。

「復元するコンピュータの選択」が表示されます。

12 コンピュータを選択し、「次へ」をクリックします。

「サマリー」が表示されます。

POINT

- 通常コンピュータは 1 台しか表示されません。

13 「次へ」をクリックします。

「ウィザードが正常に終了しました。」が表示されます。

14 「完了」をクリックします。

□ ユーザが行う作業

POINT

- 他のアプリケーションはすべて終了してください。
- 事前にユーザーキーパスワードを確認してください。
- Trusted ログオンを設定している場合は、「一時中止パスワード」にて Windows にログオンする必要があります。

1 Windows にログオンします。

2 通知領域（Windows XP の場合）またはタスクトレイ（Windows 2000 の場合）の「Broadcom Secure Fondation」のアイコンをクリックし、表示されるメニューから「Security Platform の機能の復元」を選択します。

「Broadcom Secure Foundation(TM) TPM ユーザー初期化ウィザードにようこそ」が表示されます。

3 「次へ」をクリックします。

「緊急時復元プロセス」が表示されます。

4 「基本ユーザーキーを復元する」にチェックをして、「次へ」をクリックします。

「基本ユーザーキーの復元」が表示されます。

5 自分のユーザー名を選択し、ユーザーキーの「パスワード」を入力します。

6 「次へ」をクリックします。

「基本ユーザーキーのパスワード」が表示されます。

7 「次へ」をクリックします。

「Security Platform の機能の選択」が表示されます。

8 「ユーティリティの設定を行う」の手順 14（→ P.19）以降の手順に従い、再設定します。

■通知領域またはタスクトレイから「他の OS で初期化されました」と表示された場合

□ 所有者が行う作業

1 「6 こんなときには」－「セキュリティチップの鍵を消去する」（→ P.45）の手順に従って、セキュリティチップの鍵を消去します。

2 通知領域またはタスクトレイから「Security Platform が初期化されていません。」と表示された場合」－「所有者が行う作業」（→ P.33）を行います。

□ ユーザが行う作業

1 「通知領域またはタスクトレイから「Security Platform が初期化されていません。」と表示された場合」－「ユーザが行う作業」（→ P.34）を行います。

鍵の復元について（W5200 以外の場合）

鍵の復元は、利用中のセキュリティチップにより保護された環境に何らかの変更があった場合に、以前の環境を引き続き利用するための作業です。
所有者はセキュリティチップの復元と各ユーザの復元を行う必要があります。
ユーザは、復元を行う必要はありませんが、所有者が復元を行った後にユーザーキーパスワードを入力する必要があります。
鍵の復元については、どのような状態から復元を行うかによって作業手順が異なります。
所有者でログオンした時に、通知領域（Windows XP の場合）またはタスクトレイ（Windows 2000 の場合）にメッセージが表示されます。表示される内容により、次の手順に従って処理を行ってください。

POINT

- 操作について詳しくは、Infineon Security Platform ツールのマニュアルを参照してください。

重要

- 復元処理は、セキュリティチップを設定した時のパスワードによって保護されています。そのため、復元処理はセキュリティチップを設定した人が行う必要があります。
- ほとんどの設定は「Security Platform の初期化」時および「Security Platform のユーザ初期化」時に行われます。そのときに作成したファイルを注意して管理する必要があります。また、パソコンの修理などを行う前にしておかなければならない作業もあります。手順に従い注意して管理してください。
- 手順に従ってファイルや設定変更を行わない場合、セキュリティチップで管理していた環境が利用できなくなることがあります。
- ここで説明する手順は、セキュリティチップの鍵について復元を行う場合の手順です。暗号化ファイルや証明書、および SMARTACCESE/Trust の設定については行われません。必要に応じて別途復元を行ってください。
SMARTACCESS/Trust のバックアップについては、SMARTACCESS/Trust アプリケーションのマニュアルにある「ログオン情報を移行する」を参照してください。

■通知領域またはタスクトレイから「Security Platform を復元します。」と表示された場合

□ 所有者が行う作業

1. **通知領域（Windows XP の場合）またはタスクトレイ（Windows 2000 の場合）の「Infineon Security Platform」アイコンをクリックし、表示されるメニューから「Security Platform を復元する」を選択します。**
「Infineon Security Platform 初期化ウィザードへようこそ」が表示されます。

2. **「次へ」をクリックします。**
「初期化」が表示されます。

3. **「バックアップアーカイブから Security Platform を復元する」にチェックが入っていることを確認して、「次へ」をクリックします。**
「復元」が表示されます。

4. **「新しい Trusted Platform Module」にチェックが入っていることを確認し、「復元するバックアップデータのあるファイルを指定する」にバックアップファイルが保存されている場所を指定します。**

5. **「次へ」をクリックします。**
「所有者の設定」が表示されます。

6. **「パスワード」と「パスワードの確認」に所有者のパスワードを入力し、「次へ」をクリックします。**
「トークンの選択」が表示されます。

7. **「緊急時復元用トークンの場所を指定する」に緊急時復元用トークンの保存場所を指定し、「パスワード」に設定済みのトークンのパスワードを入力します。**

8 「次へ」をクリックします。
「ユーザーの選択」が表示されます。

9 「現在のユーザー名」の「ユーザーを選択する ...」から現在のユーザを選択します。また、「ユーザ名」にユーザが表示されている場合は、それぞれのユーザの「ユーザーを選択する ...」から復元するユーザ名を選択します。

10 全ユーザの選択が完了したら、「次へ」をクリックします。
「基本ユーザーパスワード」が表示されます。

11 「パスワード」に所有者のユーザーキーパスワードを入力し、「次へ」をクリックします。
「サマリー」が表示されます。

12 表示されている内容を確認し、「次へ」をクリックします。
しばらく待つと「ウィザードが正常に終了しました。」が表示されます。

13 「Security Platform ユーザー初期化ウィザードを起動する」にチェックが入っていることを確認し、「完了」をクリックします。
「Infineon Security Platform ユーザー初期化ウィザードへようこそ」が表示されます。

14 「次へ」をクリックします。
「Security Platform の機能」が表示されます。

15 「電子メールの保護」と「暗号化ファイルシステム（EFS）によるファイルとフォルダの暗号化」をチェックして、「次へ」をクリックします。
「電子メールの保護の設定をしてください。」が表示されます。

16 「次へ」をクリックします。
「暗号化証明書」が表示されます。

17 「発行先」および「発行者」が自分になっていることを確認し、「次へ」をクリックします。
「設定を確認してください。」が表示されます。

18 表示されている内容を確認し、「次へ」をクリックします。
しばらく待つと「ウィザードが正常に終了しました。」が表示されます。

19 「完了」をクリックします。

□ ユーザが行う作業

1 Windows にログオンします。
通知領域（Windows XP の場合）またはタスクトレイ（Windows 2000 の場合）の「Infineon Security Platform」のアイコンから「キーや証明書と設定を復元します。」と表示されます。

2 **通知領域（Windows XP の場合）またはタスクトレイ（Windows 2000 の場合）の「Infineon Security Platform」のアイコンをクリックし、「Security Platform の機能を復元する」を選択します。**

「Infineon Security Platform バックアップと復元ウィザードへようこそ」が表示されます。

3 **「次へ」をクリックします。**

「基本ユーザーパスワード」が表示されます。

4 **「パスワード」にユーザーキーパスワードを入力し、「次へ」をクリックします。**

「サマリー」が表示されます。

5 **表示されている内容を確認し、「次へ」をクリックします。**

しばらく待つと「ウィザードが正常に終了しました。」が表示されます。

6 **「Security Platform ユーザー初期化ウィザードを起動する」にチェックが入っていることを確認し、「完了」をクリックします。**

「Infineon Security Platform ユーザー初期化ウィザードへようこそ」が表示されます。

7 **「所有者が行う作業」（→ P.36）の手順 12 ～ 17 を行います。**

■通知領域またはタスクトレイから「他の OS で初期化されました」と表示された場合

□ 所有者が行う作業

1 **「6 こんなときには」－「セキュリティチップの鍵を消去する」（→ P.45）の手順に従って、セキュリティチップの鍵を消去します。**

2 **「通知領域またはタスクトレイから「Security Platform を復元します。」と表示された場合」－「所有者が行う作業」（→ P.36）を行います。**

□ ユーザが行う作業

1 **「通知領域またはタスクトレイから「Security Platform を復元します。」と表示された場合」－「ユーザが行う作業」（→ P.37）の手順を行います。**

機器監査について

SMARTACCESS/Trust にて「起動時に機器監査実行」を設定しておくと、パソコンの電源を入れたときやパソコンを再起動したときにハードウェアが変更されていることを検出すると、Windows のログオンを禁止することができます。これにより、ユーザが気づかないうちに（帰宅時など）ハードウェアに何らかの変更がされても、変更されたことを検出することができます。
なお、不正にパソコンの設定が変更されたときだけでなく、修理により設定が変更された場合でも機器監査変更が検出されることがあります。修理に出す前には「パソコンの修理について」（→ P.40）を参照し、前もって設定を変更できるようにしてください。

重要

- 次に示す変更を行う場合は、前もって SMARTACCESS/Trust の「起動時に機器監査実行」をオフにし、変更した後に再度「現状登録」を行う必要があります。設定方法については、「アプリケーションの設定を行う」（→ P.25）および SMARTACCESS/Trust アプリケーションのマニュアルを参照してください。
- W5200 の場合、ハードウェアや BIOS 設定の変更を元に戻しても、機器監査の状態が元に戻らないことがあります。そのため、誤って変更してしまったり、変更後に機器監査の再登録を行わなかったりすると、Windows にログオンできなくなります。その場合は、機器構成を登録し直す必要があります。詳しい設定方法については、SMARTACCESS/Trust アプリケーションのマニュアルの「3.5 ログオンする」を参照してください。

POINT

- ハードウェアが変更されているかどうかは、休止状態からの復帰時にも確認されます。

ハードウェアの変更については以下の項目が検出されます。

□ BIOS 設定変更

BIOS にてハードウェア構成が変更された場合には、機器監査にて通知されます。

□ メモリ構成の変更

メモリスロットの構成に変更があった場合には、機器監査にて通知されます。

□ ハードディスクドライブ構成の変更（FMV-ESPRIMO シリーズの場合）

ハードディスクドライブの構成に変更があった場合には、機器監査にて通知されます（W5200 のみ）。

□ PCI スロット、グラフィックボードの変更（FMV-ESPRIMO シリーズの場合）

PCI スロットの構成およびグラフィックボードを変更した場合には、機器監査にて通知されます。

□ モバイルマルチベイ／マルチベイの変更（FMV-LIFEBOOK シリーズの場合）

モバイルマルチベイまたはマルチベイを変更した場合には、機器監査にて通知されます。

□ USB デバイスの変更（E5200 以外の場合）

USB ポートに USB メモリなどのストレージデバイスを接続した場合には、機器監査にて通知されます。

POINT

- USB デバイスの変更を検出するには、BIOS セットアップで次のように設定する必要があります。
  - ・K5200 の場合
    「USB Legacy Emulation」: Enabled
  - ・W5200、D5200 の場合
    「Legacy USB Support」: Enabled
  - ・FMV-LIFEBOOK シリーズの場合
    「レガシー USB サポート」: 使用する

  BIOS セットアップについて詳しくは、パソコン本体の『FMV マニュアル』の「BIOS」を参照してください。

パソコンの修理について

パソコンを修理に出す場合、修理後の設定が修理前とは異なることがあります。そのため、修理に出す前や出した後には次の作業が必要になります。

■修理前に必要な作業

□ 鍵のバックアップ

「鍵のバックアップについて」（→ P.29）の手順に従って、バックアップを行います。

□ Trusted ログオンを使用しない設定に変更する

機器監査を行っている場合、必ず Trusted ログオンを使用しない設定に変更してください。Trusted ログオンを使用する設定にして機器監査を行っている場合、修理したり、ハードウェアの設定を変更したりすると、Windows にログオンできなくなることがあります。

POINT

- Trusted ログオンの設定の変更については、SMARTACCESS/Trust アプリケーションのマニュアルを参照してください。

□ BIOS パスワードを解除する（W5200 以外の場合）

「4 インストールを行う」－「BIOS の設定を変更する」（→ P.12）で設定したパスワードを解除してください。

■修理後に必要な作業

□ 鍵を復元する

「鍵の復元について（W5200 の場合）」（→ P.32）または「鍵の復元について（W5200 以外の場合）」（→ P.35）の手順に従って、鍵を復元してください。

□ BIOS パスワードを設定する（W5200 以外の場合）

「4 インストールを行う」－「BIOS の設定を変更する」（→ P.12）の手順 1 ～ 6 に従って、パスワードを設定してください。

□ Trusted ログオンを使用する設定に変更する

Trusted ログオンを使用していた場合には、「4 インストールを行う」－「アプリケーションの設定を行う」（→ P.25）の手順 1 ～ 6 に従って、Trusted ログオンを使用する設定に変更してください。
なお、Trusted ログオンの設定を変更する前には、現在の機器構成を登録しておく必要があります。「4 インストールを行う」－「アプリケーションの設定を行う」（→ P.25）の手順 7 ～ 9 に従って、あらかじめ現在の機器構成を登録しておいてください。

パソコンの廃却について

パソコンを廃却する前には、安全のために、次の手順に従ってセキュリティチップの鍵や、鍵に関連するファイルを削除してください。

重要

- セキュリティチップの鍵や、鍵に関連するファイルを削除すると、セキュリティチップにより保護されていた暗号化ファイルや証明書は利用できなくなります。

1. **「6. こんなときには」－「セキュリティチップの鍵を消去する」（→ P.45）の手順に従って、セキュリティチップの鍵を消去します。**
2. **パソコン本体の『FMV　マニュアル』の「セキュリティ」－「パソコン本体廃棄時のセキュリティ」を参照して、ハードディスク内のデータを削除します。**

6 こんなときには

パスワードを変更するには

所有者パスワードまたはユーザーキーパスワードの変更は、次の方法で行います。

POINT

- セキュリティチップのパスワードは、セキュリティ面を考慮し、定期的に変更することをお勧めします。

■ W5200 の場合

□ 所有者パスワードの変更方法

1. **通知領域（Windows XP の場合）またはタスクトレイ（Windows 2000 の場合）の「Broadcom Secure Foundation」アイコンをクリックし、表示されるメニューから「Security Platform の管理」を選択します。**
   「Broadcom Secure Foundation(TM) TPM 設定ツール」が表示されます。
2. **「アドバンス」タブを選択し、「所有者のパスワード」の「変更」をクリックします。**
   以降の操作は画面の指示に従ってください。

□ ユーザーキーパスワードの変更方法

1. **通知領域（Windows XP の場合）またはタスクトレイ（Windows 2000 の場合）の「Broadcom Secure Foundation」アイコンをクリックし、表示されるメニューから「Security Platform の管理」を選択します。**
   「Broadcom Secure Foundation(TM) TPM 設定ツール」が表示されます。
2. **「ユーザー設定」タブを選択し、「基本ユーザーキーのパスワード」の「変更」をクリックします。**
   以降の操作は画面の指示に従ってください。

■ W5200 以外の場合

□ 所有者パスワードの変更方法

1. **通知領域（Windows XP の場合）またはタスクトレイ（Windows 2000 の場合）の「Infineon Security Platform」アイコンをクリックし、表示されるメニューから「Security Platform を管理する」を選択します。**
   「Infineon Security Platform 設定ツール」が表示されます。

2 **「アドバンス」タブを選択し、「所有者のパスワード」の「変更」をクリックします。**

以降の操作は画面の指示に従ってください。

□ ユーザーキーパスワードの変更方法

1 **通知領域（Windows XP の場合）またはタスクトレイ（Windows 2000 の場合）の「Infineon Security Platform」アイコンをクリックし、表示されるメニューから「Security Platform を管理する」を選択します。**

「Infineon Security Platform 設定ツール」が表示されます。

2 **「ユーザー設定」タブを選択し、「基本ユーザーパスワード」の「変更」をクリックします。**

以降の操作は画面の指示に従ってください。

パスワードを忘れた場合には

W5200 以外の場合、ユーザーキーパスワードを忘れてしまったときには、再設定することができます。
ユーザーキーパスワードを再設定する場合には、所有者により再設定を行う承認処理を行った後、各ユーザにて新しいパスワードを設定し直します。

POINT

- 操作について詳しくは、Infineon Security Platform ツールのマニュアルを参照してください。

重要

- W5200 では、ユーザーキーパスワードを忘れてしまうとパスワードを復旧することができません。パスワードを忘れないよう十分注意して管理してください。忘れてしまった場合には、「ユーザーの初期化」から再設定する必要があります。

■所有者が行う作業

1 **「スタート」ボタン→「（すべての）プログラム」→「Infineon Security Platform ソリューション」→「Security Platform を管理します」の順にクリックします。**

「Infineon Security Platform 設定ツール」が起動します。

2 **「パスワードリセット」タブをクリックし、「基本ユーザーパスワードのリセット」の「管理タスク」の「準備」をクリックします。**

「ユーザーの選択」が表示されます。

3 **ユーザーを選択し、「次へ」をクリックします。**

「トークンの選択」が表示されます。

4 「リセットトークンの場所」にリセットトークンが保存されている場所を入力し、「パスワード」に設定済みのパスワードを入力して「次へ」をクリックします。

「リセット承認コード」が表示されます。

5 「ファイルの保存」にてファイルを保存し、「次へ」をクリックします。

「ウィザードが正常に終了しました」が表示されます。

6 「完了」をクリックします。

7 保存した「リセット承認コード」ファイルと初期化時に作成した個人シークレットファイル（通常、sppwdresetsecret.xml）をユーザに渡します。

■ユーザが行う作業

1 「スタート」ボタン→「（すべての）プログラム」→「Infineon Security Platform ソリューション」→「Security Platform を管理します」の順にクリックします。

「Infineon Security Platform 設定ツール」が起動します。

2 「パスワードリセット」タブをクリックし、「基本ユーザーパスワードのリセット」の「ユーザータスク」の「リセット」をクリックします。

「リセットシークレット」が表示されます。

3 「個人シークレット」と「リセット承認コード」に所有者から受け取ったファイルを指定し「次へ」をクリックします。

「基本ユーザーパスワード」が表示されます。

4 「パスワード」と「パスワードの確認入力」に新しいパスワードを入力し「次へ」をクリックします。

「設定を確認する」が表示されます。

5 「次へ」をクリックします。

しばらく待つと、「ウィザードが正常に終了しました」が表示されます。

6 「完了」をクリックします。

セキュリティチップの鍵を消去する

パソコンを廃却する際には、パソコンに残ったデータを復元できないようにすることが重要です。セキュリティチップにより保護されたデータは、セキュリティチップ内のデータを破棄し、復元用ファイルを破棄することで再び復元することができなくなります。
セキュリティチップ内のデータを消去するには、次の手順で行います。

・「W5200 の場合」（→ P.45）
・「E5200 の場合」（→ P.46）
・「D5200、K5200 の場合」（→ P.46）
・「FMV-LIFEBOOK シリーズの場合」（→ P.47）

重要

- この操作ではセキュリティチップのデータを破棄するだけで、ハードディスクのデータは破棄されません。
- セキュリティチップのデータを破棄したことで、ハードディスク内のセキュリティチップで保護されたデータは見ることができなくなりますが、実際の廃却時にはハードディスクのデータをクリアしてください。
- BIOS セットアップで、セキュリティチップ関連の設定を行うには、管理者用パスワードを設定する必要があります（W5200 を除く）。
- BIOS セットアップについて詳しくは、パソコン本体の『FMV マニュアル』の「BIOS」を参照してください。

■W5200 の場合

1. **パソコン本体の電源を入れ、BIOS セットアップを起動します。**
BIOS セットアップ画面が表示されます。

2. **Security メニューで、【Alt】＋【S】キーを押します。**
「Clear Security Chip」の項目が設定可能になります。

3. **【↑】キーまたは【↓】キーを押して「Clear Security Chip」を選択し、【Enter】キーを押します。**
設定変更画面が表示されます。

4. **【↑】キーまたは【↓】キーを押して「Enabled」に設定します。**

5. **Exit メニューが表示されるまで、何度か【Esc】キーを押します。**

6. **【↑】キーまたは【↓】キーを押して「Save Changes & Exit」を選択し、【Enter】キーを押します。**
「Save Configuration Changes and exit now?」が表示されます。

7. **【←】キーまたは【→】キーを押して「Yes」を選択し、【Enter】キーを押します。**
BIOS セットアップが終了し、パソコン本体が再起動します。

重要

- セキュリティチップの設定を有効にするには、BIOSセットアップ終了後にパソコン本体の再起動が必要です。

■ E5200 の場合

1 **「4　インストールを行う」－「BIOS の設定を変更する」－「E5200 の場合」（→ P.13）の手順 1 ～ 6 を行います。**

2 **【↑】キーまたは【↓】キーを押して、「Clear Security Chip」を選択し、【Enter】キーを押します。**

クリアを続行してよいかを確認するウィンドウが表示されます。

3 **「Ok」を選択し、【Enter】キーを押します。**

POINT

- 完了すると「Security Chip」の設定は「Disabled」に変わります。再度「Enabled」にする場合には「4 インストールを行う」－「BIOS の設定を変更する」－「E5200 の場合」（→ P.13）の手順 7 ～ 8 を行ってください。

4 **Exit メニューが表示されるまで、何度か【Esc】キーを押します。**

5 **【↑】キーまたは【↓】キーを押して「Exit Saving Changes」を選択し、【Enter】キーを押します。**

「Save Configuration Changes and exit now?」が表示されます。

6 **【←】キーまたは【→】キーを押して「Ok」を選択し、【Enter】キーを押します。**

BIOS セットアップが終了し、パソコン本体が再起動します。

重要

- セキュリティチップの設定を有効にするには、BIOS セットアップ終了後にパソコン本体の再起動が必要です。

■ D5200、K5200 の場合

1 **「4　インストールを行う」－「BIOS の設定を変更する」－「D5200、K5200 の場合」（→ P.14）の手順 1 ～ 6 を行います。**

2 **【↑】キーまたは【↓】キーを押して、「Clear Security Chip」を選択し、【Enter】キーを押します。**

クリアを続行してよいかを確認するウィンドウが表示されます。

3 **「Yes」を選択し、【Enter】キーを押します。**

4 **Exit メニューが表示されるまで、何度か【Esc】キーを押します。**

5 【↑】キーまたは【↓】キーを押して「Exit Saving Changes」を選択し、【Enter】キーを押します。

「Save Configuration Changes and exit now?」が表示されます。

6 【←】キーまたは【→】キーを押して「Yes」を選択し、【Enter】キーを押します。

BIOS セットアップが終了し、パソコン本体が再起動します。

重要

- 「セキュリティチップ」の設定を有効にするには、BIOS セットアップ終了後にパソコン本体の再起動が必要です。終了メニューで「Exit Saving Changes」を行っただけで電源を切ってしまうと、設定が正しく行われませんのでご注意ください（次回起動時にエラーメッセージが表示されます）。

■ FMV-LIFEBOOK シリーズの場合

1 「4 インストールを行う」－「BIOS の設定を変更する」－「FMV-LIFEBOOK シリーズの場合」（→ P.15）の手順 1 ～ 6 を行います。

2 【↑】キーまたは【↓】キーを押して、「セキュリティチップのクリア」を選択し、【Enter】キーを押します。

クリアを続行してよいかを確認するウィンドウが表示されます。

3 「はい」を選択し、【Enter】キーを押します。

4 【↑】キーまたは【↓】キーを押して、「セキュリティチップ」を選択します。

5 【Space】キーまたは【－】キーを押して、「使用しない」を選択します。

6 終了メニューが表示されるまで、何度か【Esc】キーを押します。

7 【↑】キーまたは【↓】キーを押して「変更を保存して終了する」を選択し、【Enter】キーを押します。

「セットアップ確認」が表示されます。

8 【←】キーまたは【→】キーを押して「はい」を選択し、【Enter】キーを押します。

BIOS セットアップが終了し、パソコン本体が再起動します。

重要

- 「セキュリティチップ」の設定を有効にするには、BIOS セットアップ終了後にパソコン本体の再起動が必要です。終了メニューで「変更を保存する」を行っただけで電源を切ってしまうと、設定が正しく行われませんのでご注意ください（次回起動時にエラーメッセージが表示されます）。

離席時にパソコンをロックするには

コンピュータから離れる場合は、他人にコンピュータを操作されないよう注意が必要です。次の設定を行うことで、離席時でもコンピュータはセキュリティチップにより安全に保護されます。

POINT

- 各設定方法については、Windows のマニュアルを参照してください。

■スクリーンセーバーのパスワード

スクリーンセーバーを設定する際、「パスワードによる保護」を行うと、パスワードはセキュリティチップにより安全に保護されます。

■コンピュータのロック

「コンピュータのロック」（Windows XP の場合）または「ワークステーションのロック」（Windows 2000 の場合）を行うと、復帰時のパスワードはセキュリティチップにより安全に保護されます。

■スタンバイや休止状態から回復するときのパスワード

スタンバイや休止状態の設定をしている場合、「スタンバイから回復するときにパスワードの入力を求める」を設定しておくと、パスワードはセキュリティチップにより安全に保護されます。

新しいユーザを登録する

Windows に新規ユーザを追加した場合、そのユーザがセキュリティチップを利用するためには、セキュリティチップに新規ユーザの情報を登録する必要があります。

重要

- Trusted ログオンを設定している場合は、一度「一時中止パスワード」にて Windows にログオンする必要があります。所有者にご相談ください。
- 事前に Windows にユーザを追加しておく必要があります。管理者にご相談ください。
- Windows で新規ユーザを「ユーザーは次回ログオン時にパスワードの変更が必要」で作成した場合は、新規ユーザのログオン前に一度 Trusted ログオンを解除してください。Windows のパスワードを変更した後で、再度 Trusted ログオンを設定してください。

■ユーティリティへの登録

□ W5200 の場合

1 登録するユーザで、Windows にログオンします。

通知領域（Windows XP の場合）またはタスクトレイ（Windows 2000 の場合）の「Broadcom Secure Foundation」アイコンから「Security Platform の機能が初期化されていません。」というメッセージが表示されます。

2 通知領域（Windows XP の場合）またはタスクトレイ（Windows 2000 の場合）の「Broadcom Secure Foundation」アイコンをクリックします。

メニューが表示されます。

3 表示されたメニューから「Security Platform のユーザーの初期化」を選択します。

「Broadcom Secure Foundation(TM) TPM ユーザー初期化ウィザードにようこそ」が表示されます。

4 「ユーティリティの設定を行う」－「W5200 の場合」の手順 11（→ P.19）以降を行い、登録します。

5 「ユーティリティの確認を行う」－「W5200 の場合」（→ P.23）の手順で、ユーティリティが正しく設定されたか確認します。

□ W5200 以外の場合

1 登録するユーザで、Windows にログオンします。

通知領域（Windows XP の場合）またはタスクトレイ（Windows 2000 の場合）の「Infineon Security Platform」アイコンから「Security Platform の機能が初期化されていません。」というメッセージが表示されます。

2 通知領域（Windows XP の場合）またはタスクトレイ（Windows 2000 の場合）の「Infineon Security Platform」アイコンをクリックします。

メニューが表示されます。

3 表示されたメニューから「Security Platform のユーザーの初期化」を選択します。

「Infineon Security Platform ユーザー初期化ウィザードにようこそ」が表示されます。

4 「ユーティリティの設定を行う」－「W5200 以外の場合」の手順 15（→ P.21）以降を行い、登録します。

5 「ユーティリティの確認を行う」－「W5200 以外の場合」（→ P.23）の手順で、ユーティリティが正しく設定されたか確認します。

■ アプリケーションの設定

引き続き、SMARTACCESS/Trust に登録します。

1 「スタート」ボタン→「（すべての）プログラム」→「SMARTACCESS Trust」→「ログオン設定ツール」の順にクリックします。

2 ユーザーキーパスワードを入力し「次へ」をクリックします。

「ログオン設定ツール」が表示されます。

3 「Trusted ログオン」の「登録」をクリックします。

「Trusted ログオン情報登録」が表示されます。

4 Windows ログオン時の「ドメイン名」、「パスワード」、および「パスワードの確認入力」を入力します。

POINT

- ドメインを利用していない場合は、「ドメイン名」の入力は不要です。

5 「OK」をクリックします。

「Trusted ログオン情報を設定しました。」が表示されます。

6 「OK」をクリックします。

「ログオン設定ツール」に戻ります。

7 「閉じる」をクリックします。

7 トラブルシューティング

□ BIOS でセキュリティチップの設定を変更できない

BIOS で、セキュリティチップを使用するかどうかや、セキュリティチップのデータをクリアする設定を行うためには、管理者用パスワードの設定が必要です。管理者用パスワードが設定されているか確認してください。

□ ユーティリティがインストールできない

ユーティリティをインストールするには、BIOS でセキュリティチップを使用する設定になっている必要があります。BIOS の設定を確認してください。

□ SMARTACCESS/Trust が起動できない

SMARTACCESS/Trust を起動するには、ユーティリティが正常にインストールされ、初期化ウィザードとユーザー初期化ウィザードが正常に終了している必要があります。確認してください。

□ Trusted ログオン時に機器が変更された旨のエラーメッセージが表示される

前回の起動からハードウェアの構成や設定が変更された可能性があります。ハードウェア構成や BIOS 設定など変更されていないか確認してください。変更があった場合は、機器を登録したときの状態に戻してください。
なお、変更の内容によっては、機器を登録したときの状態に戻しても、エラーメッセージが解除されない場合があります。詳細は「機器監査について」（→ P.39）をご覧ください。

□ Trusted ログオン時にパスワードエラーになる

Trusted ログオンを有効にしている場合には、Windows のパスワードではなくセキュリティチップのユーザーキーパスワードを入力してください。

□ EFS が利用できない

EFS を利用するにはハードディスクが NTFS でフォーマットされていることが必要です。FAT32 のドライブでは EFS を利用することはできません。なお、Windows XP Home Edition では、EFS は利用できません。

□ セキュリティチップを「Disabled」（FMV-ESPRIMO シリーズの場合）または「使用しない」（FMV-LIFEBOOK シリーズの場合）に設定すると、Windows にログオンできなくなった

Trusted ログオンを設定した状態で、セキュリティチップを「Disabled」（FMV-ESPRIMO シリーズの場合）または「使用しない」（FMV-LIFEBOOK シリーズの場合）に設定すると、セキュリティチップにて保存していた Windows パスワードが利用できないため、Windows にログオンできなくなります。その際にはセキュリティチップを「Enabled」（FMV-ESPRIMO シリーズの場合）または「使用する」（FMV-LIFEBOOK シリーズの場合）に設定し直すか、「一時中止パスワード」にてログオンする必要があります。なお、「一時中止パスワード」でログオンしても、セキュリティチップで保護された環境は安全に管理されています。

□ ハードウェア構成を変更したために Windows にログオンできなくなった

ハードウェアの構成を変更すると、SMARTACCESS/Trust の機器監査機能により Windows にログオンできなくなります。その際にはハードウェア構成を登録したときの設定に戻すか、機器構成を登録しなおす必要があります。詳しい設定方法については、SMARTACCESS/Trust アプリケーションのマニュアルの「3.5 ログオンする」を参照してください。

□ Trusted ログオンでパスワードの入力画面が 2 度表示される

「ユーザーキーパスワード」と「一時中止パスワード」を同じにしている可能性があります。管理者にご相談ください。

□ Trusted ログオン時、内部エラー (0xe0280012) が表示される

セキュリティチップがクリアされた可能性があります。管理者にご相談ください。

□ Windows 2000 でユーザがファイルを暗号化した場合、Administrator から暗号化ファイルが読める

ファイル暗号は、Windows 標準の EFS の機能を使って行っています。Windows 2000 では EFS 暗号化を行うと、Administrator からユーザの暗号化ファイルを読むことができます。これは Windows 2000 の「回復エージェント」が Administrator になっているためです。詳しくは、Windows 2000 のマニュアルを参照してください。なお、Windows XP では、「回復エージェント」が Administrator に指定されていないため、ユーザの暗号化ファイルを読むことはできません。

□「鍵の復元について」を行うとユーザーキーパスワードが変わることがある

「5 運用上の注意」－「鍵の復元について（W5200 の場合）」（→ P.32）または「鍵の復元について（W5200 以外の場合）」（→ P.35）の手順に従って復元した場合、ユーザーキーパスワードには、バックアップを行った時点でのパスワードが設定されます。
そのため、バックアップ後にユーザーキーパスワードを変更しても、復元すると、バックアップを行った時点でのパスワードに戻ります。

□ 自動バックアップのアーカイブに全ユーザのデータが入らない場合がある（W5200 以外の場合）

パスワード変更などユーザの状態に変更があった場合は、自動バックアップにその変更が反映されるまでに時間がかかる場合があります。ユーザの状態に変更があった場合は、しばらく（30 分程度）待ってから自動バックアップを行うようにしてください。

FMV シリーズ
セキュリティチップ
取扱説明書

B6FH-6291-01 Z2-00

発 行 日　2005 年 4 月
発行責任　富士通株式会社